UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,594	12/31/2003	Ryan Charles Catherman	RPS920030206US1	8589

45503 7590 07/09/2008

DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
07/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/750,594	CATHERMAN ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-8 and 10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 5-8, 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on March 13, 2008 has been entered. Claims 1, 5-8, 10 are pending. Claims 2-4, 11, 17-24 are canceled and claim 1 is amended by the applicant.

Claim Objection

2. Claim 1 is objected to because of the following informalities:

Claim 1 recites the limitations **"the endorsement key (EK)",** "secure value that **an endorsement key** of said valid device..." are objected for lacking proper antecedent basis.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 8, 10, 11, 17-22 and 24 rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al (US Patent No. 6,892,302) in view of Kean (US Pub. No. 2002/0199110) and in view of Brickell (US Patent No. 7,142,674).

As per claim 1, Wheeler teaches:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable [col. 15 lines 57-65]; verifying

the EC (digital signature and message) [col. 16 lines 25-67]; providing/inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device [col. 17 lines 1-9, col. 18 lines 41-52]. Wheeler teaches a secure communication medium to communicate with the secure entity/credential server [Fig. 3, 1]. Wheeler teaches generating the digital signature and message for authentication/verification as above. Wheeler does not expressively mention change said first value to said second value from among: a passage of pre-set amount of device manufacturing time and a preset number of manufactured devices.

Kean teaches creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices [Fig. 2, paragraph 0012, 0191].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kean with Wheeler, since one would have been motivated to prevent reverse engineering and protect confidential information [Kean, paragraph 0028].

Wheeler teaches authentication/verification mechanism based on the digital signature and message (i.e. verifying the EC) as above. Wheeler does not expressively mention

hashing secret number with a public key and comparing the hashing values for verification.

Brickell teaches: said non-public, secure value is a secret number, forwarding a first copy of said secret number; hashing a second copy of said secret number with a public key from said endorsement key pair [col. 4 lines 29-46, Fig. 2]; combining a first hash value result from said hashing step with the public key to create the endorsement key; forwarding said EK [col. 4 lines 48-50]; verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received, said verifying step further comprising: receiving said EK from said device; hashing the public key within the received EK with the first copy of said secret number received during said forwarding step to provide a second hashed value; comparing the first hashed value from within the EK with the second hash value; and confirming said EK is from a valid device when said comparing step results in a match [Fig. 3, col. 6 lines 6-11, 12-16].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Brickell's invention with Wheeler and Kean to authenticate/verify the public key of the device, since one would have been motivated to prevent attack by man in middle attacker and provide computer security [Brickell, col. 1 lines 7-9, col. 2 lines 5-15].

As per claim 5, the rejection of claim 1 is incorporated and Wheeler teaches:

Initially storing the credential in a database of said credential server; monitoring for a request from a customer to provide said certificate to said device; and following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device [Figs. 1-6 associated text].

As per claim 6, the rejection of claim 1 is incorporated and Wheeler teaches:

It is inherent in TCPA for the endorsement key to be once writable, public readable [see TCPA Spec 1.1b, page 261] therefore it would have been obvious to one of ordinary skill in the art to make the certificate once writable, public readable.

As per claim 8, the rejection of claim 1 is incorporated and Wheeler teaches:

the credential server is remotely located a vendor manufacturing said device and said method comprises communicating said value from said device to said credential server via a secure communication medium [Fig. 1-3].

4. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al (US Patent No. 6,892,302) in view of Kean (US Pub. No. 2002/0199110) and in view of Brickell (US Patent No. 7,142,674) and in view of Wood et al (US Pub. No. 2006/0072747).

As per claim 7, the rejection of claim 1 is incorporated and Wood teaches:

using a temporary key pair [figure 6, step 605-645; paragraphs 36-39] after which the key is no longer used (discarded).

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method and system of Wheeler, Kean and Brickell with the temporary key of Wood et al. in order to provide additional security [Wood et al, paragraph 0039].

Response to Amendment

5. Applicant has amended claim 1 to include the limitations of cancelled Claims 2-4. Applicant's effort in amending the above claim has been acknowledged by the Office. However, upon further consideration, a new ground of rejection is made based on the newly found prior art. See new ground of rejection. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Wheeler et al (US 7047414) -- Managing database for reliably identifying information of device generating digital signatures

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP
7/1/08
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135